PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00, E05B 49/00

A1

(11) International Publication Number: **WO 98/26534**

(43) International Publication Date: 18 June 1998 (18.06.98)

(21) International Application Number: PCT/US97/18814

(22) International Filing Date: 15 October 1997 (15.10.97)

(30) Priority Data:
08/758,530 29 November 1996 (29.11.96) US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: FINKELSTEIN, Louis, D.; 1698 W. Ottowa, Wheeling, IL 60090 (US). DABBISH, Ezzat; 445 Adare Drive, Cary, IL 60013 (US). HIRKA, Gerald, M.; 2322 W. Rice Street, Chicago, IL 60622 (US).

(74) Agents: HOPMAN, Nicholas, C. et al.; Motorola Inc., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

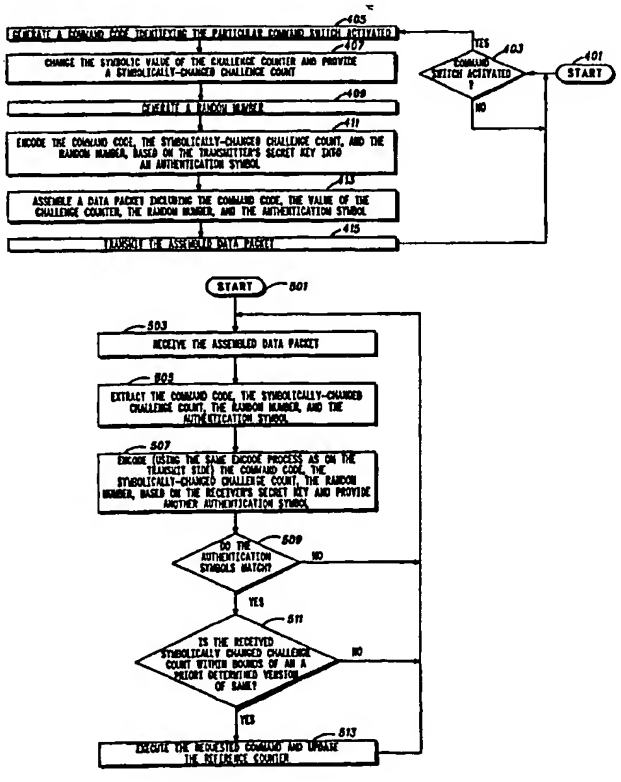
(81) Designated States: JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: AUTHENTICATION SYSTEM AND METHOD FOR A REMOTE KEYLESS ENTRY SYSTEM

(57) Abstract

An authentication system and method changes (407) a symbolic value of a challenge count and encodes (411) it into an authentication symbol using an encoding process. Then, the symbolically-changed challenge count and the authentication symbol are transmitted (415). When received, the symbolically-changed challenge count is encoded (507) using the encoding process, and a receive-side derived authentication symbol is formed therefrom. Authentication is indicated (511) when the authentication symbol and the receive-side derived authentication symbol match.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

AUTHENTICATION SYSTEM AND METHOD FOR A REMOTE KEYLESS ENTRY SYSTEM

Field of the Invention

This invention is related to the field of remote keyless entry systems for use in vehicular applications and more particularly to an authentication system and method therefor.

Background of the Invention

Contemporary vehicle's often employ Remote Keyless Entry (RKE) systems that include control functions such as those to unlock doors of the vehicle, start the engine in the vehicle, or to open a garage door. Typically radio signals are transmitted from an RKE transmitter which is typically a portable device, to an RKE receiver which is typically mounted in a vehicle or in a garage. When the radio signals are transmitted, it is feasible, using electronic eavesdropping, to record the radio signals for later re-transmission to operate the control functions of the vehicle or the garage door opener.

To dissuade unauthorized access, RKE systems are made more secure by digitally encoding the radio signals transmitted between the RKE transmitter and the RKE receiver. Before the digitally encoded radio signals received by the RKE receiver can be used, their origin needs to be validated. This validation process is often called authentication.

While various authentication methods and systems exist they are inadequate because they lack sufficient security to prevent unauthorized use of the RKE system. A secure system must prevent against playback attack, cryptoanalysis attack, and be resistant to cloning. To be considered secure, a change of one symbol bit induced by a command query should result in a change of at least half of the symbol bits transmitted. If this happens the system is said to have the avalanche effect - which is good. Current RKE transmission schemes inadequately address the security issue.

What is needed is an improved approach to authentication for RKE systems that is more secure than prior implementations.

Brief Description of the Drawings

FIG. 1 is a system block diagram of a transmitter side of a Remote Keyless Entry (RKE) system in accordance with a preferred embodiment of the invention;

FIG. 2 is a system block diagram of a receiver side of the RKE system in accordance with the preferred embodiment of the invention;

FIG. 3 is a schematic block diagram of the RKE system;

FIG. 4 is a flow chart showing a preferred method of transmitter portion of an RKE system; and

FIG. 5 is a flow chart showing a preferred method of receiver side authentication in an RKE system.

Detailed Description of a Preferred Embodiment

An authentication system method changes a symbolic value of a challenge count and encodes it into an authentication symbol using an encoding process. Then, the symbolically-changed challenge count and the authentication symbol are transmitted. When received, the symbolically-changed challenge count is encoded using the encoding process, and a receive-side derived authentication symbol is formed therefrom. Authentication is indicated when the authentication symbol and the receive-side derived authentication symbol match. Essentially, if an authentication symbol formed in a transmitter-side process matches an authentication symbol formed in a receiver-side process, then there must have been an authentic transmission and reception. Since the challenge count is changed with every new transmission and reception, a high level of security against a potential theft and use of the transmitted and received information is achieved. Furthermore, to increase the security against playback performance, a random number is combined with the challenge count before it is first encoded. Further security features will be introduced later with the introduction of figures covering the specific structures of the invention.

FIG. 1 is a system block diagram of a transmitter side of a Remote Keyless Entry (RKE) system. RKE systems are often provided for automobiles as part of a convenience package. The RKE system enables a driver to lock and unlock doors of the vehicle while the driver is in close proximity to the vehicle. Also, as an added

convenience, some RKE systems allow the driver to remotely start his or her car.

FIG. 1 illustrates how the RKE transmitter collects and transmits its control information to the receiver located in the vehicle. Command switches 101, located on a hand-held RKE transmitter device 100, typically include an UNLOCK switch, a LOCK switch, a TRUNK RELEASE switch, and an ENGINE START switch, and may include other switches such as an ALARM switch. When one of the command switches is activated, a switch encoder 103 encodes it and provides a command switch code 105, indicative of which of the command switches is activated. Also, when the command switch is activated, a challenge counter 107 changes its symbolic value and provides a symbolically-changed challenge count 109. In a simple case the challenge counter 107 would merely be incremented. In a more complex application, the symbolic value of the challenge counter would change to another value; as long as the new value is pre-agreed-to, or computed, by both the transmitter side and the receiver side of the RKE system. This action of always changing the symbolic value of the challenge counter provides a certain level of security to the system.

To further increase the security of the system, a random number 111 is generated by a random number generator 113 that is used to further decrease the predictability and increase the complexity of the system. Also, many vehicle manufacturers prefer to include a unit identification number 115 (or unit ID). This unit ID can be conveniently generated by extracting it from a memory, such as a

Electrically Erasable Programmable Read Only Memory 117 (EEPROM) located on the RKE transmitter.

Before transmitting the switch command code 105, the symbolically-changed challenge count 109, the random number 111, and the unit ID 115, these data are used to generate an authentication symbol 121 using an encoder 123, and a unique secure, or secret key 125 provided by the EEPROM 117. The encoder 123 can take many forms but it essentially hashes, whitens, or encrypts the data using the unique secret key 125.

As with many robust transmission schemes a CRC or Cyclic Redundancy Check symbol 127 is computed based on the switch command code 105, the symbolically-changed challenge count 109, the random number 111, and the unit ID 115, and the authentication symbol 121. The CRC symbol 127 is then combined or joined with the switch command code 105, the symbolically-changed challenge count 109, the random number 111, and the unit ID 115, and the authentication symbol 121 to form an assembled data packet, or message 129 which is then transmitted using a transmitter 131. Alternatively a MAC or Message Authentication Code may be used instead of a CRC method.

FIG. 2 is a system block diagram of a receiver side of a RKE system. FIG. 2 illustrates by what means the RKE receiver collects and acts on the collected information to activate action in the vehicle.

A scheduler 201, located in an RKE control system 200, controls the operation of several of the system's 200 elements. At the request of the scheduler 201, a receiver 202 receives the assembled data

packet 129 transmitted by the transmitter 131, introduced in FIG. 1. For efficiency reasons the unit ID 115 is extracted from the assembled data packet 129 and compared to a receiver-side EEPROM 209 derived unit ID 215. If these two IDs match, then a unit ID match 217 is indicated. If the two IDs do not match, then the scheduler 201 aborts any operations of other control system 200 elements. Then, the scheduler 201 waits a predetermined amount of time and then again requests another assembled data packet 129 from the receiver. The predetermined amount of time that the scheduler 201 waits is determined based on a rate of transmission of the assembled data packet 129. This delay is necessary to prevent the system 200 from being tied up in continuously processing the assembled data packet 129 while the received unit ID 115 knowingly does not match the receiver-side EEPROM 209 derived unit ID 215.

If the unit ID match 217 is indicated, then the scheduler commands a CRC check circuit 203 to extract the he CRC symbol 127 from the assembled data packet 129 and to validate the integrity of the transmission and reception. If a valid CRC symbol 127 was not received, then the CRC check circuit 127 alerts the scheduler 201. The scheduler 201 then waits the predetermined amount of time and then again requests another assembled data packet 129 from the receiver.

If a valid CRC symbol 127 was transmitted and received, then the switch command code 105, the symbolically-changed challenge count 109, and the random number 111 are extracted from the assembled data packet 129, and with a secret, or secure key 207 provided by a

receiver-side EEPROM 209, a receive-side derived authentication symbol 211 is derived in the encoder 205. Note that the receiver-side encoder 205 operates exactly in the same way that the encoder 123 operates on the transmitter side of the RKE system, and the secret key 207 is identical to the transmitter-side key 125.

Once encoded, the receive-side derived authentication symbol 211 is compared with the authentication symbol 121 received from the transmitter 131 in block 224. If the two symbols match, then a match is indicated 213. If the two symbols do not match, then the block 224 alerts the scheduler 201. The scheduler 201 then waits the predetermined amount of time and then again requests another assembled data packet 129 from the receiver.

If block 224 indicated a match, then the symbolically-changed challenge count 109, received by the receiver 202 is compared to an a priori determined (base) challenge count 219. If the received symbolically-changed challenge count 109 matches 221 (within a predetermined bounds as determined by block 223) the a priori determined base challenge count 219, then the a priori determined base challenge count 219 is updated (preferably made the same as - but not necessarily) to have a symbolic value equal to the symbolically-changed challenge count 109.

If the received symbolically-changed challenge count 109 does not match the a priori determined (base) challenge count 219, then the block 223 alerts the scheduler 201. The scheduler 201 then waits the predetermined amount of time and then again requests another assembled data packet 129 from the receiver.

In system block 225, if a match is indicated between the receive-side derived authentication symbol 211 and the authentication symbol 121 as indicated at reference number 213, and (optionally) the unit IDs match as indicated at reference number 217, and received symbolically-changed challenge count 109 matches the a priori determined base challenge count 219 as indicated at reference number 221 then authentication is indicated and the switch command code 105, received by the receiver 202, is executed in the vehicle.

Now that the overall system has been described a hardware platform will be detailed. FIG. 3 is a schematic block diagram of the RKE system. The hand-held RKE transmitter device 100, includes a transmit controller 301, which interprets the command switches 101, and, after executing the preferred method, transmits the assembled data packet 129 using its transmitter 131. The transmit controller 301 can be constructed using digital circuitry, a microcontroller, or any other mechanism which essentially performs a portion of the preferred method. In the preferred embodiment a Motorola MC68HC05 microcontroller will be used. The Motorola MC68HC05 microcontroller has on-board program memory used to store the portion of the preferred method described later, and an EEPROM facility for the EEPROM 117 described earlier.

The RKE control system 200 includes a receiver controller 303 which executes another portion of the preferred method. The receiver controller 303 includes an actuator drive circuit 305, and a microcontroller 307. According to the preferred method, the receiver controller 303 receives the assembled data packet 129 using

its receiver 202. The microcontroller 307, again preferably a Motorola MC68HC05 microcontroller with on-board program memory to store the portion of the preferred method described later, and an EEPROM facility for the EEPROM 209 described earlier, interprets the assembled data packet 129 and commands the actuator drive 305 to drive external actuators. These external actuators include door lock solenoids and engine starting devices. Now that the hardware platform has been detailed, the preferred method steps for both the RKE transmitter device 100, and the RKE control system 200 will be introduced.

FIG. 4 is a flow chart showing a preferred method of transmitter portion of an RKE system, and FIG. 5 is a flow chart showing a preferred method of receiver side authentication in an RKE system. Note that these flow charts are essentially encoded into each of the Motorola MC68HC05 microcontrollers of the controllers 301 and 307 respectively.

Commencing with FIG. 4, the Motorola MC68HC05 microcontroller, of the transmit controller 301 embedded within the RKE transmitter device 100, invokes a transmitter-side portion of the preferred method.

In step 403 the microcontroller determines whether or not a command switch, has been activated. If a command switch has been activated, then, in step 405 a switch command code identifying the particular command switch activated is generated.

Next, in step 407 a symbolic value of a challenge count is changed, and a symbolically-changed challenge count is provided in

response to the generation of the switch command code resulting from the command switch activation. In a simple case, the challenge count is essentially a binary counter maintained within a register of the microcontroller. In this example the symbolic value is simply the arithmetic value of the counter. So, if at a particular moment the arithmetic value of the counter is 345, and a command switch is activated, the counter is incremented by one, and therefore the symbolically-changed challenge count is now 346. Of course, other symbolic representations and/or incremental values can be used.

In step 409 the microcontroller generates a random number. Then, in step 411 the switch command code, the symbolically-changed challenge count, and the random number are encoded into an authentication symbol using an encoding process. Optionally, for more security, a unit ID, stored in the microcontroller's EEPROM can also be included in the data that is encoded. The encoding process is effected using a secret key also stored in the microcontroller's EEPROM. The encoding process can take the form of any process that predictably alters the essential form of the raw data. Preferably, this encoding process is an encryption process, but can also take the form of a filtering, whitening, or other data-altering process.

Next, in step 413 a data packet is formed and includes the unit ID, the random number, the symbolically-changed challenge count, the switch command code, and the authentication symbol. Preferably, a CRC (or MAC) symbol is computed based on the symbolic values of the unit ID, the random number, the symbolically-changed challenge

count, the switch command code, and the authentication symbol and is then included forming an assembled data packet to be transmitted.

Then, in step 415, the assembled data packet is transmitted by the transmitter 131. Essentially, the method described in FIG. 4, executed on the microcontroller embedded within the transmit controller 301 of the RKE transmitter device 100 emulates the system block diagram introduced in FIG. 1. Next, FIG. 5 will be described.

A receiver-side portion of the preferred method commences at a start step 501. Next, in step 503, the assembled data packet transmitted by the transmitter 131 is received by the receiver 202 and passed to the microcontroller 307. As indicated earlier in FIG. 2, the CRC symbol 127 is checked for validity. If valid, in step 505 the unit ID, the random number, the symbolically-changed challenge count, and the switch command code are extracted from the data packet and are encoded in step 507 based on the receiver-side secret key to form a receive-side derived authentication symbol 211.

Next, in accordance with the system block diagram in FIG. 2, in step 509 a test is made to see whether or not the received authentication symbol 121, and the receive-side derived authentication symbol 211 match. This could be an exact symbolic match, or a symbolic match within some pre-agreed-to bounds. Authentication can be indicated at this time. To make the method more robust another step 511 can be added.

For instance, if the symbols match, then in step 511 the symbolically-changed challenge count received in the step of receiving is compared to an a priori determined base challenge count. If the

symbolically-changed challenge count is different (in a pre-agreed-to way - like one symbolic count larger, or smaller), then authentication can be indicated. If authentication is indicated, then the a priori determined base challenge count can be updated based on the symbolically-changed challenge count received in the step of receiving 503.

Optionally, as described in FIG. 2 a match of unit IDs can also be used in the authentication process. Once authentication is indicated in step 511, in step 513, the command, indicated by the switch command code received in the step of receiving 503, is executed by having the microcontroller 307 control the actuator drive 305 which in turn unlocks a vehicle door or whatever the command is programmed to do.

Although the RKE control system 200 described here relies on one unit ID, one could easily use several unit IDs. In this case, each ID would be associated with a different secret key.

In conclusion the improved approach to authentication for RKE systems that is more secure than prior implementations. Novel improvements include an authentication approach that is secure because of transmission of a non-repeating code. Moreover, with the addition of the random number, the system and method will decrease the predictability and increase the complexity of the transmission and reception process which significantly improves the security of this approach over prior art schemes.

What is claimed is:

Claims

1. An authentication method comprising the steps of:

changing a symbolic value of a challenge count and providing a symbolically-changed challenge count responsive thereto;

providing a unique secret key;

encoding the symbolically-changed challenge count into an authentication symbol using an encoding process dependent on the unique secret key;

transmitting the symbolically-changed challenge count and the authentication symbol;

receiving the symbolically-changed challenge count and the authentication symbol;

encoding the symbolically-changed challenge count received in the step of receiving using the encoding process dependent on the unique secret key, and forming a receive-side derived authentication symbol therefrom; and

indicating authentication when the authentication symbol received in the step of receiving, and the receive-side derived authentication symbol match.

2. A method in accordance with claim 1 wherein the step of indicating comprises a step of:

indicating authentication when the authentication symbol received in the step of receiving, and the receive-side derived authentication symbol have a symbolically equivalent symbolic value.

3. A method in accordance with claim 1 wherein the step of changing a symbolic value of a challenge count comprises a step of:

increasing a symbolic value of the challenge count and providing a symbolically-changed challenge count.

4. A method in accordance with claim 1 wherein the step of changing a symbolic value of a challenge count comprises a step of:

decreasing a symbolic value of the challenge count and providing a symbolically-changed challenge count.

5. A method in accordance with claim 1 wherein the step of indicating comprises a step of:

indicating authentication when the authentication symbol received in the step of receiving, and the receive-side derived authentication symbol have a symbolically equivalent symbolic value, and the symbolic value of the symbolically-changed challenge count received in the step of receiving, has a symbolic value bounded within a predetermined proximity of an a priori determined base challenge count.

6. A method in accordance with claim 5 further comprising a step of:

replacing the a priori determined base challenge count with the symbolically-changed challenge count received in the step of receiving, responsive to the step of indicating authentication.

7. A method in accordance with claim 5 wherein the predetermined proximity is defined as greater than the symbolic value of the a priori determined base challenge count, and less than five symbolic values greater than the symbolic value of the a priori determined base challenge count.

8. An authentication method comprising the steps of:

changing a symbolic value of a challenge count and providing a symbolically-changed challenge count responsive thereto;

generating a random number;

encoding the symbolically-changed challenge count and the random number into an authentication symbol using an encoding process;

forming a data packet comprising the symbolically-changed challenge count, the random number, and the authentication symbol;

transmitting the data packet;

receiving the data packet;

extracting the symbolically-changed challenge count, and the random number, received in the step of receiving the data packet;

encoding the symbolically-changed challenge count and the random number, both extracted in the step of extracting, using the encoding process, and forming a receive-side derived authentication symbol therefrom; and

indicating authentication when the authentication symbol received in the step of receiving, and the receive-side derived authentication symbol match.

9. A method in accordance with claim 8 wherein the step of indicating comprises a step of:

indicating authentication when the authentication symbol received in the step of receiving, and the receive-side derived authentication symbol have a symbolically equivalent symbolic value.

10. A method in accordance with claim 9 wherein the step of changing a symbolic value of a challenge count comprises a step of:

increasing a symbolic value of the challenge count and providing a symbolically-changed challenge count.

11. A method in accordance with claim 8 wherein the step of changing a symbolic value of a challenge count comprises a step of:

decreasing a symbolic value of the challenge count and providing a symbolically-changed challenge count.

12. A method in accordance with claim 9 wherein the step of indicating comprises a step of:

indicating authentication when the authentication symbol received in the step of receiving, and the receive-side derived authentication symbol have a symbolically equivalent symbolic value, and the symbolic value of the symbolically-changed challenge count received in the step of receiving, has a symbolic value bounded within a predetermined proximity of an a priori determined base challenge count.

13. A method in accordance with claim 12 further comprising a step of:

replacing the a priori determined base challenge count with the symbolically-changed challenge count received in the step of receiving, responsive to the step of indicating authentication.

14. A method in accordance with claim 8 further comprising the step of:

activating a command switch, and generating a command code responsive thereto; and

wherein the step of changing a symbolic value of a challenge count comprises a step of changing a symbolic value of a challenge count responsive to the step of generating a command code, and wherein the step of forming a data packet comprises a step of forming a data packet comprising the symbolically-changed challenge count, the authentication symbol, and the command code.

15. A method in accordance with claim 8 further comprising the step of:

providing a unique secret key; and

wherein the step of encoding the symbolically-changed challenge count into the authentication symbol comprises encoding the symbolically-changed challenge count into an authentication symbol using an encoding process dependent on the unique secret key, and the step of encoding the symbolically-changed challenge count received in the step of receiving comprises encoding the symbolically-changed challenge count received in the step of receiving using the encoding process dependent on the unique secret key, and forming the receive-side derived authentication symbol therefrom.

16. An authentication method for a secure remote keyless entry system comprising the steps of:

activating a command switch, and generating a command code responsive thereto;

changing a symbolic value of a challenge count and providing a symbolically-changed challenge count in response to the generation of the command code resulting from the step of activating;

generating a random number;

providing a unique secret key;

encoding the symbolically-changed challenge count, the command code, and the random number into an authentication symbol using an encoding process dependent on the unique secret key;

forming a data packet comprising the random number, the command code, the symbolically-changed challenge count, and the authentication symbol;

transmitting the data packet;

receiving the data packet;

encoding the symbolically-changed challenge count, the command code, and the random number, received in the step of receiving, using the encoding process dependent on the unique secret key, and forming a receive-side derived authentication symbol therefrom; and

indicating authentication when the authentication symbol received in the step of receiving, and the receive-side derived authentication symbol have a symbolically equivalent symbolic value, and the symbolic value of the symbolically-changed challenge count received

in the step of receiving, has a symbolic value larger than an a priori determined base challenge count.

17. A portable transmission device comprising:

a command switch for generating a command code responsive to activation thereof;

a symbolic counter, operatively coupled to the command switch, the counter for changing a symbolic value of a challenge count and providing a symbolically-changed challenge count responsive to the activation of the command switch;

a random number generator for generating a random number;

an encoder, coupled to the symbolic counter, the encoder providing an authentication symbol dependent on the symbolically-changed challenge count provided by the symbolic counter and the random number;

a device for joining the command code, the symbolically-changed challenge count, the random number, and the authentication symbol into a data message;

a transmitter for transmitting the data message;

a receiver, for receiving the transmitted data message;

another encoder, coupled to the receiver, the encoder for encoding the symbolically-changed challenge count, and the random number received by the receiver, and forming a receive-side derived authentication symbol therefrom; and

a device for indicating authentication when the authentication symbol received by the receiver, and the receive-side derived authentication symbol have a symbolically equivalent value, and the symbolic value of the symbolically-changed challenge count received

by the receiver, has a symbolic value larger than an a priori determined base challenge count.

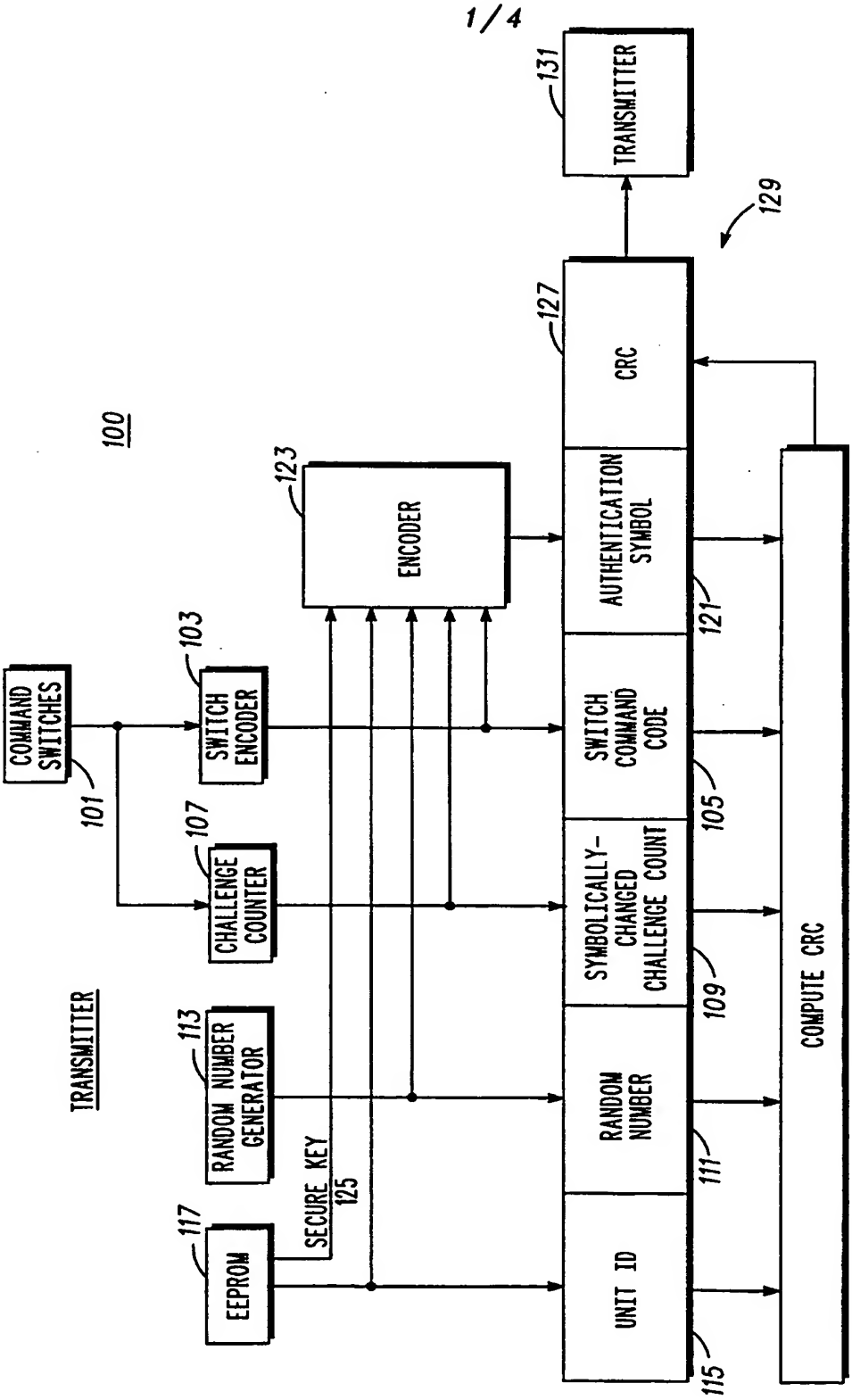

100
TRANSMITTER
COMMAND SWITCHES
101
SWITCH ENCODER
103
CHALLENGE COUNTER
107
RANDOM NUMBER GENERATOR
113
SECURE KEY
125
EEPROM
117
ENCODER
123
TRANSMITTER
131
129
CRC
127
AUTHENTICATION SYMBOL
121
SWITCH COMMAND CODE
105
SYMBOLICALLY-CHANGED CHALLENGE COUNT
109
RANDOM NUMBER
111
UNIT ID
115
COMPUTE CRC

FIG.1

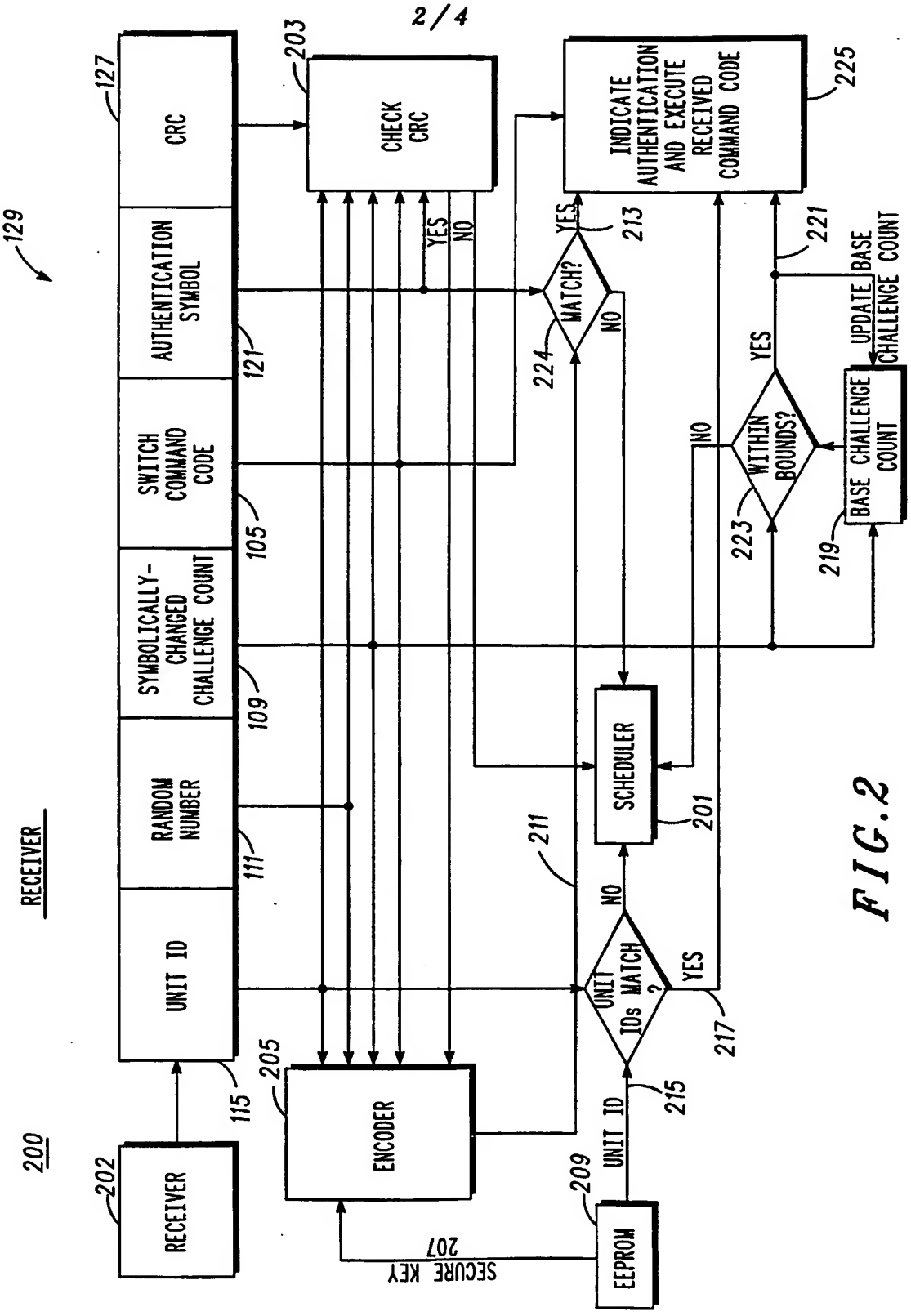

200
RECEIVER
129
127
CRC
AUTHENTICATION SYMBOL
SWITCH COMMAND CODE
SYMBOLICALLY-CHANGED CHALLENGE COUNT
RANDOM NUMBER
UNIT ID
121
105
109
111
115
202
RECEIVER
205
ENCODER
207
SECURE KEY
209
EEPROM
UNIT ID
203
CHECK CRC
YES
NO
213
MATCH?
224
211
SCHEDULER
201
UNIT IDs MATCH ?
215
217
NO
YES
225
INDICATE AUTHENTICATION AND EXECUTE RECEIVED COMMAND CODE
221
UPDATE BASE CHALLENGE COUNT
WITHIN BOUNDS?
223
BASE CHALLENGE COUNT
219

FIG. 2

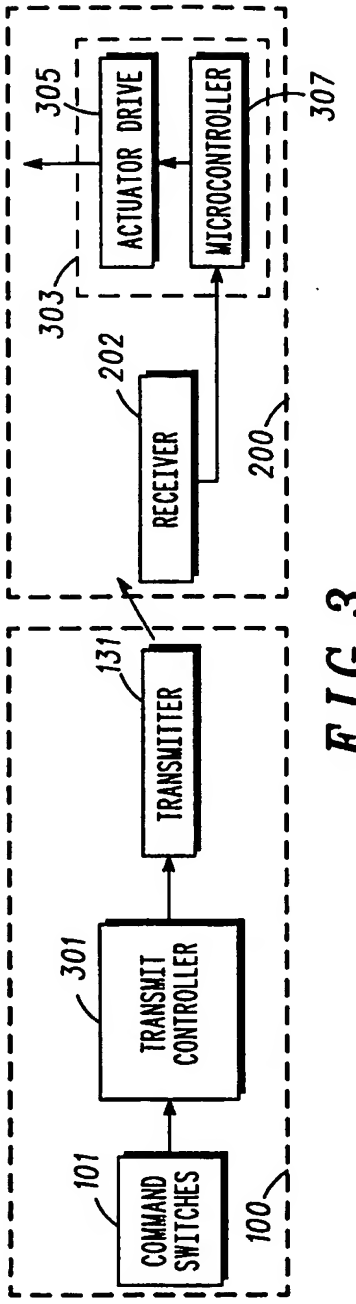

100
101
COMMAND SWITCHES
301
TRANSMIT CONTROLLER
131
TRANSMITTER
200
202
RECEIVER
303
305
ACTUATOR DRIVE
307
MICROCONTROLLER

FIG.3

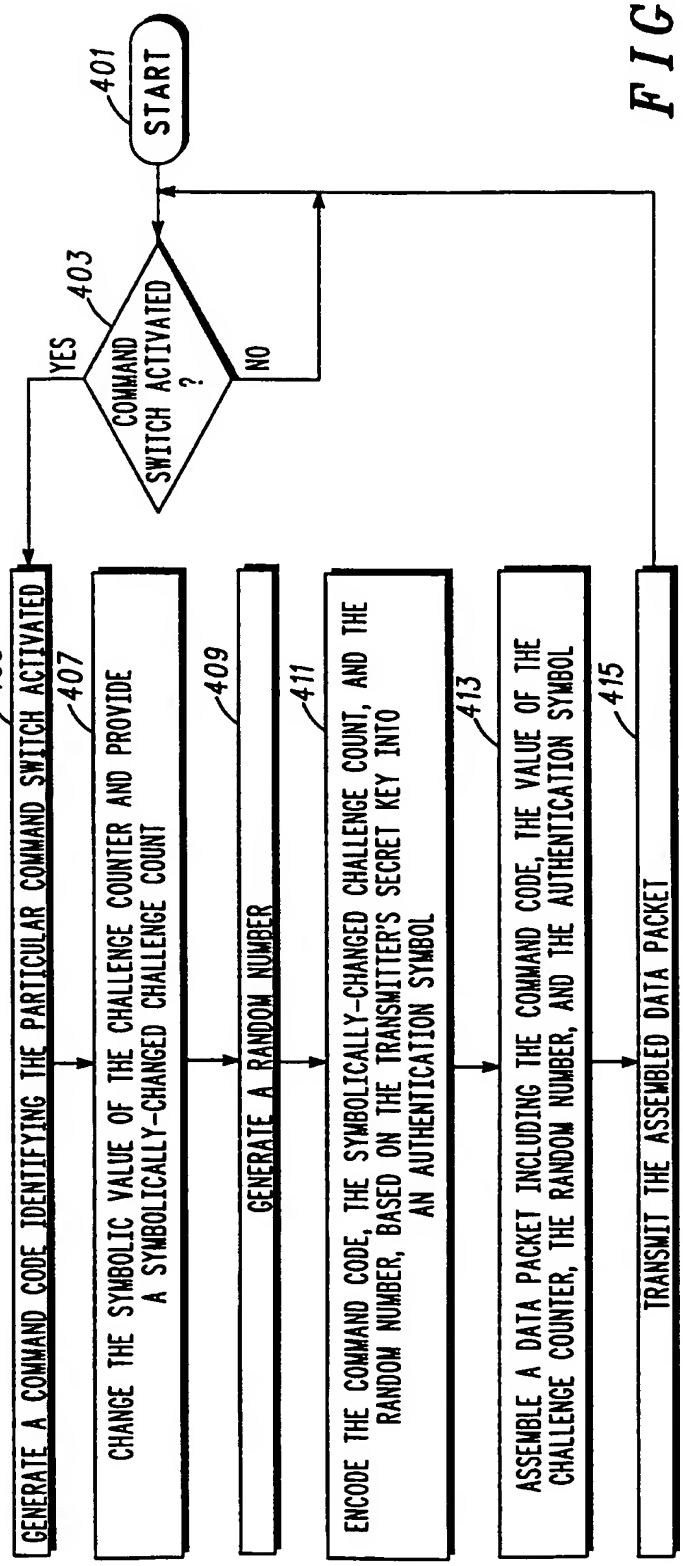

401
START
403
COMMAND SWITCH ACTIVATED ?
YES
NO
405
GENERATE A COMMAND CODE IDENTIFYING THE PARTICULAR COMMAND SWITCH ACTIVATED
407
CHANGE THE SYMBOLIC VALUE OF THE CHALLENGE COUNTER AND PROVIDE A SYMBOLICALLY-CHANGED CHALLENGE COUNT
409
GENERATE A RANDOM NUMBER
411
ENCODE THE COMMAND CODE, THE SYMBOLICALLY-CHANGED CHALLENGE COUNT, AND THE RANDOM NUMBER, BASED ON THE TRANSMITTER'S SECRET KEY INTO AN AUTHENTICATION SYMBOL
413
ASSEMBLE A DATA PACKET INCLUDING THE COMMAND CODE, THE VALUE OF THE CHALLENGE COUNTER, THE RANDOM NUMBER, AND THE AUTHENTICATION SYMBOL
415
TRANSMIT THE ASSEMBLED DATA PACKET

FIG.4

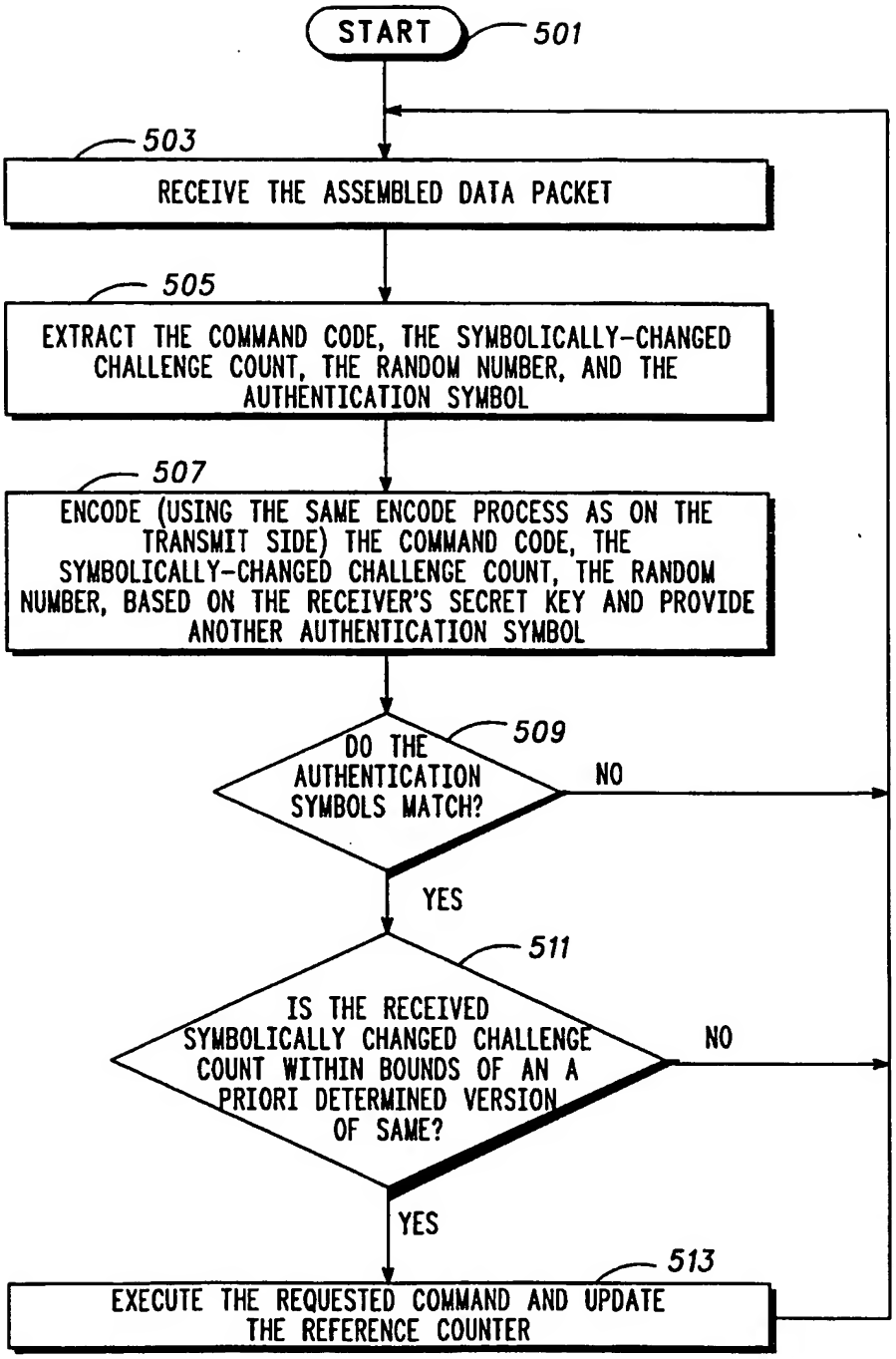

START
501
503
RECEIVE THE ASSEMBLED DATA PACKET
505
EXTRACT THE COMMAND CODE, THE SYMBOLICALLY-CHANGED CHALLENGE COUNT, THE RANDOM NUMBER, AND THE AUTHENTICATION SYMBOL
507
ENCODE (USING THE SAME ENCODE PROCESS AS ON THE TRANSMIT SIDE) THE COMMAND CODE, THE SYMBOLICALLY-CHANGED CHALLENGE COUNT, THE RANDOM NUMBER, BASED ON THE RECEIVER'S SECRET KEY AND PROVIDE ANOTHER AUTHENTICATION SYMBOL
509
DO THE AUTHENTICATION SYMBOLS MATCH?
NO
YES
511
IS THE RECEIVED SYMBOLICALLY CHANGED CHALLENGE COUNT WITHIN BOUNDS OF AN A PRIORI DETERMINED VERSION OF SAME?
NO
YES
513
EXECUTE THE REQUESTED COMMAND AND UPDATE THE REFERENCE COUNTER

FIG.5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/18814

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00; E05B 49/00;
US CL :380/23; 340/825.31, 825.34;
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23, 25; 340/825.31, 825.34; 307/10.2

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS search terms: keyless entry

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 5,420,925 A (MICHAELS) 30 May 1995 - Entire, See Abstract	8, 9, 11, 12 --- 4,5, 7, 15-17
X -- Y	US 5,144,667 A (POGUE, JR. et al.) 01 September 1992 -entire	1-3 --- 4,5, 7, 16-17
X -- Y	US 5,191,610 A (HILL et al.) 02 March 1993 - Abstract	8 -- 5
X,P	US 5,619,573 A (BRINKMEYER et al.) 08 April 1997 - entire; see col. 1 and claims	1-7

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"B"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
01 MAY 1998

Date of mailing of the international search report
28 MAY 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
PINCHUS M.LAUFER
Telephone No. (703) 306-4177

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/18814

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 5,708,712 A (BRINKMEYER et al.) 13 January 1998- entire, see figures 1 and 3	1-17